Amendments to the Specification

Please replace the paragraph at page 26, line 17 - page 28, line 15 with the following amended paragraph:

In Figure 2, the processing starts at step 201. It is presumed that a projective coordinate component X_0 of the x-coordinate of a given point R and a scalar value m are inputted and that a projective coordinate component X_m of the x-coordinate of a point corresponding to m-multiple of R is to be outputted. On this assumption, the scalar value m and the projective coordinate component X_0 of the x-coordinate are inputted (step 202). In the succeeding steps 203 to 205, data stirring is performed by multiplying the individual projective coordinates by the random number. More specifically, the random number k is generated in the step 203, whereon k^2X_0 is arithmetically determined by multiplying the projective coordinate component X_0 by the random number k and assigned to X_1 in the step 204 while the random number k itself is assigned to Z_1 in the step 205. In succeeding steps 206 to 208 and 301, preparation is made for the scalar multiplication. In more concrete, $[X_1, Z_1]$ is assigned to $[X_4, Z_4]$ in the step 206, being followed by the step 206 where $[X_1, Z_1]$ is inputted to the doubling process (illustrated in Fig. 5), the output of which is then assigned to $[X_2, Z_2]$ in the step 207. Further, in a step 208, the scalar value m is transformed to a binary bit string $h_i h_{i-1} \ldots h_0$, where the most significant bit h_1 is "1" and thus "1" is assigned to i in a step 301 shown in Fig. 3. Through processing steps 302 to 309 (see Fig. 3), the addition method and the doubling method are controlled in dependence on whether one bit of the scalar value m is "0" or "1" to

thereby realize the scalar multiplication. More specifically, "i-1" is assigned to i in the step 302, which is followed by the step 303 where $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$ are inputted to the addition process (illustrated in Fig. 4), the output of which is assigned to $[X_3, Z_3]$ in the step 303. At this juncture, when $h_i == 0$ (i.e., when the step 304 results in affirmation "Yes"), the processing proceeds to the step 305 while it proceeds to the step 307 when $h_i == 1$, i.e., when the decision step 304 results in negation "No". In the step 305, $[X_1, Z_1]$ is inputted to the doubling arithmetic or process (Fig. 5), the output from which is assigned to $[X_1, Z_1]$. In the step 306, $[X_3, Z_3]$ is assigned to $[X_2, Z_2]$, whereon the processing proceeds to the step 309. On the other hand, when the decision step 304 results in "No", $[X_2, Z_2]$ is inputted to the doubling arithmetic or process illustrated in Fig. 5, the output of which is assigned to $[X_2, Z_2]$ (step 307). In the step 308, $[X_3, Z_3]$ is assigned to $[X_1, Z_1]$, whereupon the processing proceeds to the step 309. In the case where $i > 0$, i.e., the step 309 results in "Yes", when the step 302 is resumed. If otherwise, i.e., when the decision step 309 results in "No", the processing proceeds to a step 310. Subsequently, the projective coordinates are transformed to the x-coordinate of the (x, y) coordinate system. Finally $X_1/(Z_1)^2$ is assigned to the projective coordinate component X_m (step 310) to be ultimately outputted (step 311). The processing ends at step 312.

Please replace the paragraph at page 30, line 5 - page 31, line 10 with the following amended paragraph:

Figure 4 is a flow chart for illustrating the addition method according to the first embodiment of the present invention. Processing starts at step 401. The

projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$ are inputted, whereby coordinates $[X_3, Z_3]$ or a point at infinity is outputted. Thus, the projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$ are inputted in a step 402. Through processings in steps 403 to 407, $X_1(Z_2)^2 + X_2(Z_1)^2$ is determined for making decision whether or not the result of the addition arithmetic represents the point at infinity. Interim results S_1, S_2 and B provide preparation for the realization of the expressions (2) and (3) mentioned above. More specifically, $X_1(Z_2)^2$ is assigned to S_1 in the step 403 and $X_2(Z_1)^2$ is assigned to S_2 in the step 404 whereupon $S_1 + S_2$ is assigned to B in the step 405. When B == 0 in the step 406 (i.e., when the decision step 406 results in "Yes"), the processing proceeds to the step 407. If otherwise (i.e., when the decision in the step 406 results in "No"), the processing proceeds to the step 408. In the step 407, the point at infinity is outputted, whereon the processing comes to an end (step 413). Through the processing steps 408 to 411 executed when the decision step 406 results in "No", the coordinates $[X_3, Z_3]$ are determined in accordance with the expressions (2) and (3) mentioned hereinbefore. In more concrete, Z_4B is assigned to Z_3 in the step 408 and $(Z_4)^2S_1S_2$ is assigned to S in the step 408 with X_4B^2 being assigned to M in the step 410, whereupon M + S is assigned to X_3 in the step 411, and $[X_3, Z_3]$ is outputted in the step 412. Through the procedure described above, the addition arithmetic can be realized sextuple multiplications of the mutually different variables. In other words, X_3 can be arithmetically determined from X_1, X_2 and X_4 at a high speed. The process ends at step 413.

Please replace the paragraph at page 31, line 27 - page 32, line 28 with the following amended paragraph:

Figure 5 is ~~as flow chart~~ a flowchart for illustrating the doubling method according to the first embodiment of the present invention. Referring to the figure, step 501 denotes start. ~~It~~ It is presumed that $Q = [X_1, Z_1]$ and b are inputted, whereby $2Q = [X_2, Z_2]$ or alternatively the point at infinity is to be outputted. In a step 502, X_1 and Z_1 are inputted. In the succeeding steps 503 and 504, decision is made whether or not $X_1 == 0$ or $Z_1 == 0$ is valid in order to make decision as to whether the doubling arithmetic results in the point at infinity. Namely, when $X_1 == 0$ or $Z_1 == 0$ in the step 503 (i.e., when the decision step 503 results in "Yes"), the processing step proceeds to the step 504. If otherwise (i.e., when the decision step 503 results in "No"), the processing proceeds to a step 505. In the step 504, the point at infinity is outputted. In the succeeding steps 505 to 507, the coordinates $[X_2, Z_2]$ are determined in accordance with expressions (4) and (5) mentioned previously. More specifically, in the step 505, Z_1^2 is assigned to S. In the step 506, X_1S is assigned to Z_2. In the step 507, $X_1^4 + b(S)^4$ is assigned to X_2 (step 507). In the step 508, the coordinates $[X_2, Z_2]$ are outputted. Through the procedure described above, the addition arithmetic can be realized by executing twice the multiplication of mutually different variables. Accordingly, in the scalar multiplication method, the addition arithmetic can be realized by executing (6 + 2 = 8) - times the multiplication of mutually different variables per bit of the scalar value d. In other words, the

A3

projective coordinate X_3 can be arithmetically determined very speedily from X_1, X_2 and X_4. The process ends at step 509.

Please replace the paragraph at page 34, line 28 - page 36, line 22 with the following amended paragraph:

Figures 6 and 7 in combination illustrate in a flow chart, a processing procedure for the scalar multiplication method according to the second embodiment of the present invention. The process begins at step 601. It is presumed that a projective coordinate component X_0 of the x-coordinate of a given point R and a scalar value m are inputted for thereby outputting a projective coordinate component X_m of the x-coordinate of a point corresponding to the m-multiplication or m-tuple of R. To this end, the scalar value m and the projective coordinate component X_0 of the x-coordinate are inputted in the step 602. In the succeeding steps 603 and 604, transformation of X_0 to the projective coordinate is performed. More specifically, in the step 603, X_0 is assigned to X_1. In the step 604, "1" is assigned to Z_1. In the processing steps 605 to 607, preparation is made for the scalar multiplication. In more concrete, coordinates $[X_1, Z_1]$ are assigned to $[X_4, Z_4]$ in the step 605 to thereby allow $[X_1, Z_1]$ to be inputted to the doubling arithmetic (Fig. 5), the output of which is assigned to $[X_2, Z_2]$ in the step 606. In the step 607, $h_i h_{i-1} \ldots h_0$ are set as the binary bit string representing the scalar value m, in which the most significant bit h_1 is "1", and thus "1" is assigned to i in a step 701 shown in Fig. 7. In the succeeding processing steps 702 to 709, the addition method and the doubling method are controlled in dependence on whether one bit of the scalar value m is "0"

A4

or "1", to thereby determine the scalar multiplication. More specifically, in the step 702, "i-1" is assigned to i while in the step 703, $[X_1, Z_1]$, $[X_2, Z_2]$ and X_0 are inputted to the addition method (Fig. 8), the output of which is assigned to $[X_3, Z_3]$. When $h_i == 0$ (i.e., when the decision step 704 results in affirmation "Yes"), the processing proceeds to the step 707 when $h_i == 1$, i.e., when the decision step 704 results in negation "No". In the step 705, $[X_1, Z_1]$ is inputted to the doubling method (Fig. 5), the output from which is assigned to $[X_1, Z_1]$. In the succeeding step 706, $[X_3, Z_3]$ is assigned to $[X_2, Z_2]$, whereupon the processing proceeds to the step 709. On the other hand, in the step 707, $[X_2, Z_2]$ is inputted to the doubling method (Fig. 5), the output of which is assigned to $[X_2, Z_2]$. In the succeeding step 708, $[X_3, Z_3]$ is assigned to $[X_1, Z_1]$, whereupon the processing proceeds to the decision step 709. In case the decision step 709 results in that $i > 0$ (i.e., when the step 709 results in "Yes"), the step 702 is resumed. On the other hand when $i \leq 0$, i.e., when the decision step results in "No", the processing proceeds to step 710 where $X_1/(Z_1)^2$ is assigned to the projective coordinate component X_m to be ultimately outputted (step 711). The process ends at step 712.

Please replace the paragraph at page 36, line 24 - page 37, line 24 with the following amended paragraph:

Figure 8 is a flow chart for illustrating the addition method according to the second embodiment of the invention. Step 801 denotes start. It is presumed that the projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$ are inputted and that $[X_3, Z_3]$ or the point at infinity is to be outputted. Thus, the projective coordinates $[X_1, Z_1]$,

$[X_2, Z_2]$ and $[X_4, Z_4]$ are inputted in a step 802. Through the processings in subsequent steps 803 to 807, $X_1(Z_2)^2 + X_2(Z_1)^2$ is computed for making decision whether or not the result of the addition represents the point at infinity. Interim results S_1, S_2 and B provide preparation for realization of the expressions (6) and (7) mentioned previously. More specifically, $X_1(Z_2)^2$ is assigned to S_1 in the step 803. In the step 804, $X_2(Z_1)^2$ is assigned to ~~S_2. in the~~ S_2. In the step 805, $S_1 + S_2$ is assigned to B. When it is decided that B == 0 in the step 806 (i.e., when decision in the step 806 results in "Yes"), the processing proceeds to the step 807. If otherwise (i.e., when the decision in the step 806 results ~~in "No~~in "No"), the processing proceeds to the step 808. In the step 807, the point at infinity is outputted, whereon the processing proceeds to the step 813. Through the processing steps 808 to 811, the projective coordinates $[X_3, Z_3]$ are determined in accordance with the expressions (6) and (7) mentioned hereinbefore. In more concrete, B is assigned to Z_3 in the step 808. In the step 809, S_1S_2 is assigned to S. In the step 810, $X_4Z_3^2$ is assigned to M. In the step 811, M + S is assigned to X_3. Finally, in the step 812, $[X_3, Z_3]$ is outputted. Step 813 denotes end.

Please replace the paragraph at ~~page~~ 40, ~~line~~ 16 ~~page~~ 42, ~~line~~ 14 with the following amended paragraph:

Figures 11A and 11B are flow charts for illustrating the scalar multiplication method in which the Montgomery method is adopted according to the third embodiment of the present invention. Referring to the figures, ~~it~~ the process starts at step 1101. It is presumed that a projective coordinate component X_0 of the x-

coordinate of a given point R and a scalar value m are inputted and that a projective coordinate component X_m of the x-coordinate of a point corresponding to m-multiplication of R is to be outputted. To this end, the scalar value m and the projective coordinate component X_0 of the x-coordinate are inputted in the step 1102 shown in Fig. 11A. In the succeeding steps 1103 to 1105, data is stirred through multiplication of the individual coordinates in the projective coordinate system by the random number. More specifically, the random number k is generated in step 1103, whereon kX_0 is determined by multiplying the projective component X_0 of the x-coordinate by the random number k, and then kX_0 is assigned to X_1 in the step 1104 while the random number k being assigned to Z_1 in the step 1105. In succession, $[X_1, Z_1]$ is assigned to $[X_4, Z_4]$ (step 1106). Subsequently, $[X_1, Z_1]$ is inputted to the doubling method (i.e., Montgomery's doubling arithmetic), the output of which is assigned to $[X_2, Z_2]$ (step 1107). Further, the scalar value m is transformed to the binary bit string $h_i h_{i-1} \ldots h_0$ (step 1108), where the most significant bit h_1 is "1". Thus "1" is assigned to i in the step 1109 shown in Fig. 11B. In a succeeding step 1110, "i-1" is assigned to i, which is then followed by a step 1111 where $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$ are inputted to the addition method (Montgomery's addition arithmetic), the output of which is assigned to $[X_3, Z_3]$ (step 1111). When $h_i == 0$ in the step 1112 (i.e., when the decision step 1112 results in affirmation "Yes), the processing proceeds to a step 1113 while it proceeds to a step 1115 when $h_i == 1$, i.e., when the decision step 1112 results in negation "No". In the step 1113 shown in Fig. 11B, $[X_1, Z_1]$ is inputted to the doubling method (Montgomery's doubling arithmetic), the output

from which is assigned to $[X_1, Z_1]$. In the succeeding step 1114, $[X_3, Z_3]$ is assigned to $[X_2, Z_2]$, whereon the processing proceeds to a step 1117. On the other hand, when the decision step 1112 results in "No", $[X_2, Z_2]$ is inputted to the doubling method (Montgomery's doubling arithmetic), the output of which is assigned to $[X_2, Z_2]$ (step 1115). Further, $[X_3, Z_3]$ is assigned to $[X_1, Z_1]$ in the step 1116, whereupon the processing proceeds to a step 1117. In the case where $i > 0$, i.e., the step 1117 results in "Yes", the step 1110 is resumed. If otherwise, i.e., when the decision step 1117 results in "No", the processing proceeds to a step 1118 where $X_1/(Z_1)$ is assigned to the projective coordinate component X_m to be ultimately outputted in the step 1119, whereupon the processing comes to an end (step 1120).

A6

Please replace the paragraph at page 43, line 26 - page 45, line 21 with the following amended paragraph:

Figures 12A and 12B are flow charts for illustrating the scalar multiplication method according to the fourth embodiment of the present invention. Referring to the figures, ~~it~~ the process starts at step 1201. It is presumed that a projective coordinate component X_0 of the x-coordinate of a given point R and a scalar value m are inputted and that a projective component X_m of the x-coordinate of a point corresponding to m-multiplication of R (i.e., the point corresponding to the product of m and R) is to be outputted. On the presumption, the scalar value m and the projective coordinate component X_0 of the x-coordinate are inputted in the step 1202 shown in Fig. 12A. In the succeeding steps 1203 to 1205, data is stirred through multiplication of the individual projective coordinates by the random number. More

A7

specifically, the random number k is generated in the step 1203, whereon kX_0 is determined by multiplying the projective coordinate component X_0 of the x-coordinate by the random number k, and then kX_0 is assigned to X_1 in the step 1204 while the random number k itself being assigned to Z_1 in the step 1205. In succession, $[X_1, Z_1]$ is assigned to $[X_4, Z_4]$ (step 1206). Subsequently, $[X_1, Z_1]$ is inputted to the doubling arithmetic, the output of which is assigned to $[X_2, Z_2]$ (step 1207). Further, the scalar value m is transformed to the binary bit string $h_i\ h_{i-1} \ldots h_0$ (step 1208), where the most significant h_1 is "1". Thus, "1" is assigned to i in the step 1209 shown in Fig. 12B. In a succeeding step 1210, "i - 1" is assigned to i, which is then followed by a ~~step 1011~~ step 1211 where $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$ are inputted to the addition arithmetic, the output of which is assigned to $[X_3, Z_3]$. When h_i == "0" in the step 1212 (i.e., when he decision step 1212 results in affirmation "Yes"), the processing proceeds to a step 1213 while it proceeds to a step 1215 when h_i == "1", i.e., when the decision step 1212 results in negation "No". In the step 1213 shown in Fig. 12B, $[X_1, Z_1]$ is inputted to the doubling arithmetic, the output from which is assigned to $[X_1, Z_1]$. In the succeeding step 1214, $[X_3, Z_3]$ is assigned to $[X_2, Z_2]$, whereon the processing proceeds to a step 1217. On the other hand, when the decision step 1212 results in "No", $[X_2, Z_2]$ is inputted to the doubling arithmetic, the output of which is assigned to $[X_2, Z_2]$ (step 1215). Further, $[X_3, Z_3]$ is assigned to $[X_1, Z_1]$ in the step 1216, whereupon the processing proceeds to a step 1217. In the case where $i > 0$, i.e., when the step 1217 results in "Yes", the step 1210 is resumed. If otherwise, i.e., when the decision step 1217 results in "No", the

A7

processing proceeds to a step 1218 where $X_1/(Z_1)$ is assigned to the projective coordinate component X_m to be ultimately outputted in the step 1219, whereupon the processing comes to an end (step 1220).

Please replace the paragraph at page 47, lines 2-22 with the following amended paragraph:

Figure 13 is a flow chart for illustrating an addition method according to the fourth embodiment of the present invention. The process starts at step 1301. It is assumed that projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$ are inputted, whereby $[X_3, Z_3]$ or the point at infinity is outputted. Thus, projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$ are inputted in a step 1302. Subsequently X_1Z_2 is assigned to S_1 in a step 1303. Further, X_2Z_1 is assigned to S_2 in a step 1304, whereon $S_1 + S_2$ is assigned to B in a step 1305. When B == 0 in a step 1306 (i.e., when decision in the step 1306 results in "Yes"), the processing proceeds to a step 1307. If otherwise (i.e., when the decision in the step 1306 results in "No"), the processing proceeds to a step 1308. In the step 1307, the point at infinity is outputted, and then a step 1313 is executed. On the other hand, when the decision step 1306 results in "No", Z_4B^2 is assigned to Z_3 in a step 1308. Further, $(Z_4)^2S_1S_2$ is assigned to S in a ~~step 1309,~~ ~~Subsequently~~step 1309. Subsequently, X_4B^2 is assigned to M in a step 1310 while M + S is assigned to X_3 in a step 1311, whereon $[X_3, Z_3]$ is outputted in a step 1312.

A8

Please replace the paragraph at page 48, line 16 - page 49, line 4 with the following amended paragraph:

Figure 14 is a flow chart for illustrating a doubling method according to the fourth embodiment of the invention. The processing starts at step 1401. It is presumed that $Q = [X_1, Z_1]$ and b are inputted for thereby outputting $2Q = [X_2, Z_2]$ or the point at infinity. More specifically, $[X_1, Z_1]$ and b are inputted in a step 1402. When $X_2 == 0$ or $Z_2 == 0$ (i.e., when the decision in the step 1403 results in "Yes"), the processing proceeds to a step 1404. If otherwise (i.e., when the decision step 1403 results in "No"), the processing proceeds to the step 1405. In the step 1404, the point at infinity is outputted. In the step 1405, Z_1^2 is assigned to Z_2. In the step 1406, X_1^2S is assigned to S. In the step 1407, $X_1^4 + bS$ is assigned to X_2, which is then followed by a step 1408 where $[X_2, Z_2]$ is outputted. Through the procedure described above, the addition arithmetic can be realized by executing twice the multiplication of mutually different variables. The process ends at step 1409.

A9

Please replace the paragraph at page 51, line 25 - page 52, line 26 with the following amended paragraph:

Figure 16 is a flow chart for illustrating an addition method according to the fifth embodiment of the present invention. The process starts at step 601. It is assumed that projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and X_4 are inputted, whereby $[X_3, Z_3]$ or the point at infinity is outputted. Thus, projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and X_4 are inputted in a step 1602. In the succeeding step 1603, X_1Z_2 is assigned to S_1. Further, X_2Z_1 is assigned to S_2 in a step 1604 with $S_1 + S_2$ being assigned to B in a step 1605. When B == 0 in a step 1606 (i.e., when decision in the step 1606 results in "Yes"), the processing proceeds to a step 1607. If otherwise

A10

(i.e., when decision in the step 1606 results in "No), the processing proceeds to a step 1608. In the step 1607, the point at infinity is outputted, whereon an end step 1613 is executed. On the other hand, unless B = 0 in the step 1606, B^2 is assigned to Z_3 (step 1608). In the succeeding ~~step 1608~~step 1609, S_1S_2 is assigned to S. Further, (X_4Z^3) is assigned to M in a step 1610 while M + S is assigned to X_3 in a step 1611. Finally, $[X_3, Z_3]$ is outputted in a step 1612. The process ends at step 1613. Through the procedure described above, the addition arithmetic can be realized by executing four times the multiplication of mutually different variables. Parenthetically, as the doubling arithmetic according to the instant embodiment of the invention, the doubling arithmetic described hereinbefore can be adopted. Additionally, the method incarnated in the instant embodiment can also find application not only to the arithmetic with the elliptic curve in the finite field of characteristic 2 but also to the arithmetic with the elliptic curve in the prime field.

A10

Please replace the paragraph at ~~page~~ 53, ~~line~~ 24 - ~~page~~ 55, ~~line~~ 6 with the following amended paragraph:

The elliptic curve arithmetic unit 901 has input 902 and output 903 and includes a random number generation module 904 for generating a random number k to be outputted, as indicated by an arrow 905. The random number k generated by the random number generation module 904 is inputted to a projective coordinate transformation module 906 together with the x-coordinate X_0, the scalar value m and the parameter b although they are not shown in Fig. 9, to be thereby transformed to the projective coordinates $[kX_0, k]$, which is then assigned to $[X_1, Z_1]$. The projective

A11

coordinate [X_1, Z_1] and the scalar value m are inputted to a scalar multiplication module 908 (arrow 907), whereby a point given by [X_1, Z_1] multiplied by m is determined. Thus, the x-coordinate X_m of the point as determined is outputted from the scalar multiplication module 908 (arrow 912). In the scalar multiplication module 908, [X_1, Z_1] is first assigned to [X_4, Z_4] which may be previously stored in a memory incorporated, for example, in the scalar multiplication module. Further, the projective coordinates [X_1, Z_1] are supplied to a doubling arithmetic module 913 for determining a double point [X_2, Z_2]. Subsequently, m is developed to a binary bit string. Every time the bit assumes "0", starting the more significant bit, [X_1, Z_1] is supplied to the doubling arithmetic 913, whereon the double point outputted from the doubling arithmetic module 913 is assigned to [X_1, Z_1] (arrow 914). Subsequently, projective coordinates [X_1, Z_1], [X_2, Z_2] and [X_4, Z_4] are inputted to an addition arithmetic module 910 (arrow 909), and the addition point outputted from the addition arithmetic module 910 is assigned to [X_2, Z_2] (arrow 911). On the other hand, when the bit is "1", the projective coordinates [X_2, Z_2] are outputted to the doubling arithmetic module 913, whereon the double point outputted from the doubling arithmetic module 913 is assigned to [X_2, Z_2]. Subsequently, the projective coordinates, [X_1, Z_1], [X_2, Z_2] and [X_4, Z_4] are inputted to the addition arithmetic module 910, and the addition point outputted from the addition arithmetic module 910 is assigned to [X_1, Z_1]. Thus, there is derived the X_m-coordinate of the m-tuple point.